Electronic Version
Stylesheet Version v1.1.1

Intrusion Detection

Abstract

A system daemon starts through normal system startup procedures and reads its configuration file to determine which data entities (e.g., directories and files) are to be monitored. The monitoring includes a valid MD5 signature, correct permissions, ownership of the file, and an existence of the file. If any modification are made to the data entities, then the system daemon generates an alarm (intended for the administrator of the host) that an intrusion has taken place. Once an intrusion is detected, then the isolating steps or commands are issued in a real-time continuous manner to protect the host system from attack or intrusion.